The State of Ransomware. Trends and Mitigation Techniques

Alexander Adamov
NioGuard Security Lab,
Kharkiv National University of Radioelectronics
oleksandr.adamov@nure.ua

Anders Carlsson
Blekinge Institute of Technology,
anders.carlsson@bth.se

Abstract

This paper contains an analysis of the payload of the popular ransomware for Windows, Android, Linux, and MacOSX platforms. Namely, VaultCrypt (CrypVault), TeslaCrypt, NanoLocker, Trojan-Ransom.Linux.Cryptor, Android Simplelocker, OSX/KeRanger-A, WannaCry, Petya, NotPetya, Cerber, Spora, Serpent ransomware were put under the microscope. A set of characteristics was proposed to be used for the analysis.

The purpose of the analysis is generalization of the collected data that describes behavior and design trends of modern ransomware.

The objective is to suggest ransomware threat mitigation techniques based on the obtained information.

The novelty of the paper is the analysis methodology based on the chosen set of 13 key characteristics that helps to determine similarities and differences thorough the list of ransomware put under analysis. Most of the ransomware samples presented were manually analyzed by the authors eliminating contradictions in descriptions of ransomware behavior published by different malware research laboratories through verification of the payload of the latest versions of ransomware.

1. Introduction

The discussion on ransomware and cryptolockers is not new and started in 1996 [1]. In 2005, the capability of using MS Crypto API to create "cryptovirus" was described in [2]. Since 2010, when the first unbreakable GpCode cryptolocker, which used RSA-1024 to encrypt a session RC4 key, was discovered by Kaspersky Lab [3], it has been noticed significant progress in cryptolockers design [4]. C&C servers and decryption services have moved into the Tor network making it impossible to trace and take down a server [5]. Web decryption services now look like a real customer service desk hosted in the Tor network as well. Criminals started using Bitcoins as an anonymous payment service. Elliptic curves cryptography has come together with bitcoins. For example, TeslaCrypt [6] used ECDH to generate a bitcoin address and as a carrier for a session AES key.

The existing researches in ransomware shows whether the lack of malware analysis expertise or ransomware samples used for analysis are out of date and cannot be met in-the-wild. For example, in [7] the authors analyzed 1,359 samples that belong to 15 different ransomware families using . However, as stated in the paper, all the samples were in the wild between 2006 and 2014, which means the proposed mitigation strategies address the attacks that were not active by 2015, when the paper was published.

In this work, the typical samples of the popular ransomware for Windows, Linux, MacOSX, and Android platforms discovered during the last years were analyzed covering almost all possible infection cases. Moreover, the Cerber [8], Spora [9], Serpent [10], Petya [11], WannaCry [12], and NotPetya [13] were active at the moment of writing this paper. The Cerber, Spora, and Serpent families are in continues development.

2. A Ransomware Analysis Methodology

We analyzed the latest discovered cryptolockers found in the wild since 2014 until the present moment that belong to the following families: TeslaCrypt [6], VaultCrypt (CrypVault, BAT_CRYPVALT.A) [14], NanoLocker [15], Trojan-Ransom.Linux.Cryptor (Linux.Cryptor, Linux.Encoder.1) [16, 17], and Android Simplelocker [18], OSX/KeRanger-A[19], Petya [11], WannaCry [12], NotPetya [13], Cerber [8],

978-1-5386-3299-4/17/$31.00 ©2017 IEEE

Spora [9], Serpent[10]. Note, that a verdict name may vary depending on a security vendor detected a corresponding threat. We selected a set of key characteristics which we were considering during the ransomware analysis. These characteristics include:

- delivery method
- file type
- platform
- files encryption method
- session key (used to encrypt files) encryption method
- encryption locations
- deleting backup
- communication with C&C server
- decryption service location
- payment information
- target audience
- passive methods of self-protection
- active methods of self-protection

3. The Results of Ransomware Analysis

The results of ransomware analysis are summarized below and provided by the selected criteria.

3.1. Delivery method

This subsection presents the delivery method used by the ransomware samples under analysis.

VaultCrypt: via spam messages with a malicious javascript attachment
TeslaCrypt: landed via a drive-by attack with the help of the Angler web exploit [20]
NanoLocker: no information available
Linux.Cryptor: via exploitation of a vulnerability in the Magento platform to launch attacks on web servers
Simplelocker: downloaded from unofficial Android app stores as a fake porn game
OSX/KeRanger-A: via hacked website
WannaCry: EternalBlue exploit
Petya: CVE-2017-0199 exploit in RTF
NotPetya: EternalBlue and EternalRomance exploits
Cerber: spear-phishing email
Spora: spear-phishing and watering hole attacks
Serpent: spear-phishing

3.2. Platform / File type

This subsection presents the target platform and file type of the ransomware samples under analysis.

VaultCrypt: Windows/BAT
TeslaCrypt: Windows/EXE
NanoLocker: Windows/EXE
Linux.Cryptor: Linux/ELF
Simplelocker: Android/APK
OSX/KeRanger-A: MacOSX
WannaCry: Windows/EXE
Petya:Windows/EXE
NotPetya:Windows/EXE
Cerber: Windows/EXE
Spora: Windows/EXE
Serpent: Windows/EXE

3.3. Files encryption method

This subsection presents the file encryption methods used by the ransomware samples under analysis. The ransomware sample uses the Windows Enhanced Cryptographic Provider (RSAENH) if other is not specified.

VaultCrypt: RSA-1024 using the GnuPG tool
TeslaCrypt: AES-256-CBC using OpenSSL
NanoLocker: AES-256-CBC
Linux.Cryptor: AES-128-CBC using PolarSSL
Simplelocker: AES-128-CBC using cryptolib
OSX/KeRanger-A: AES-256-CBC
WannaCry: AES-128-CBC
Petya: encrypts MFT with Salsa20-256
NotPetya: AES-128-CBC, encrypts MFT with Salsa20-256
Cerber: RC4-128
Spora: AES-256-CBC
Serpent: AES-256-CBC

3.4. Encryption method for a session or file key

This subsection presents encryption method used to encrypt a session or file key preventing locked files from decryption. A cryptolocker generates a new session key for every its run in a user's environment. The session key can be used directly to encrypt all files or encrypts individual file encryption keys. In case of using a session key for individual file's keys, a file's key encrypted by a session key is usually stored in a file's header/footer (Cerber, Spora).

VaultCrypt: RSA-1024 with the hard-coded master public key using GnuPG tool
TeslaCrypt: the files encryption key is used as a multiplier in the calculated ECDH shared secret sent to

the C&C server and stored in a header of encrypted files.

NanoLocker: RSA-1024 with the hard-coded master public key and base64 encoded to be sent via a Public Note in a Bitcoin transaction

Linux.Cryptor: RSA-1024 with the hard-coded master public key

Simplelocker: the files' encryption key is hard-coded "jndlasf074hr"

OSX/KeRanger-A: RSA-2048 to encrypt a random seed used for AES

WannaCry: RSA-2048

Petya: the custom algorithm

NotPetya: RSA-2048

Cerber: RSA-880 and RSA-2048

Spora: RSA-1024

Serpent: RSA-2048

3.5. Encryption locations

This subsection describes encryption locations used by the ransomware samples under analysis.

VaultCrypt: except Windows, msoffice, Intel, and framework64

TeslaCrypt: except Windows, Program Files, and Application Data. The files are encrypted in shared folders and removable drives as well

NanoLocker: n/a

Linux.Cryptor: files are encrypted in the folders: /home, /root, /var/lib/mysql, /var/www, /etc/nginx, /etc/apache2, /var/log

Simplelocker: files on an SD card

OSX/KeRanger-A: Users, Volumes

WannaCry: except \\, $\, Intel, ProgramData, WINDOWS, Program Files, Program Files (x86), AppData\Local\Temp, Local Settings\Temp, Temporary Internet Files, Content.IE5

Petya: MFT

NotPetya: MFT

Cerber: except $getcurrent, $recycle.bin, $windows.~bt, $windows.~ws, boot, documents and settings\all users\, documents and settings\default user, documents and settings\localservice, documents and settings\networkservice, intel, msocache, perflogs program files (x86), program files, programdata, recovery, recycled, recycler, system volume information, temp, windows.old, windows10upgrade, windows, winnt, appdata\local, appdata\locallow, appdata\roaming, local settings, public\music\sample music, public\pictures\sample pictures, public\videos\sample videos, tor browser

Spora: except appdata, games, program files, program files (x86), windows.

Serpent: except program files (x86), program files, tor browser, windows, programdata, $recycle.bin

3.6. Deleting backup

This subsection shows if the analyzed ransomware deletes backup copies of the files, for example, shadow copies.

VaultCrypt: uses SDelete [21] or Cipher tools [22] to wipe the keys files

TeslaCrypt: yes, using vssadmin.exe [23] to delete shadow copies of files

NanoLocker: n/a

Linux.Cryptor: n/a

Simplelocker: n/a

OSX/KeRanger-A: encrypt Time Machine backup files

WannaCry: uses vssadmin.exe [23] to delete shadow copies of files

Petya: n/a

NotPetya: n/a

Cerber: n/a

Spora: uses vssadmin.exe [23] to delete shadow copies of files

Serpent: uses WMIC [24] and Cipher [22] tools to delete shadow copies and wipe the original files from a disk

3.7. Communication with a C&C server

This subsection points to a C&C communication protocol used by ransomware, if any.

VaultCrypt: http://revault.me

TeslaCrypt: URL varies on the build version, data transmitted in an encrypted way (AES-256-CBC) with the hard-coded key

NanoLocker: ICMP, two ping packets are sent with a Bitcoin address to C&C (52.91.55.122), the second ping packet is sent once the encryption is completed and also contains the number of encrypted files

Linux.Cryptor: n/a

Simplelocker: C&C in Tor (http://xeyocsu7fu2vjhxs.onion/), user's data are transmitted in JSON format

OSX/KeRanger-A: over the Tor network

WannaCry: over the Tor network

Petya: n/a

NotPetya: n/a

Cerber: CIDRs are used (77.12.57.0/27, 19.48.17.0/27, 87.98.176.0/22) to find a C&C server, remote port 6893
Spora: over the Tor network
Serpent: hmkwegza.pw, pwmhgfhm.pw, over the Tor network

3.8. Decryption service

This subsection describes where an online decryption service is located, if any.

VaultCrypt: in the Tor network
TeslaCrypt: in the Tor network
NanoLocker: using a Public Note in Bitcoin transaction
Linux.Cryptor: in the Tor network
Simplelocker: the decrypting function is available in the cryptolocker's code
OSX/KeRanger-A: in the Tor network
WannaCry: in the Tor network
Petya: in the Tor network
NotPetya: n/a
Cerber: in the Tor network
Spora: spora.bz, in the Tor network
Serpent: in the Tor network

3.9. Payment

This subsection gives an overview of ransom payments demanded by ransomware.

VaultCrypt: in BTC, the price depen
ds on the number of encrypted files
TeslaCrypt: $500 equivalent in BTC, doubled every 60 hours
NanoLocker: 0.25 BTC
Linux.Cryptor: 1 BTC
Simplelocker: MoneXy, Qiwi
OSX/KeRanger-A: 1 BTC
WannaCry: $300/600 in BTC
Petya: $300/600 in BTC
NotPetya: n/a
Cerber: 0.045/0.090 BTC
Spora: depends on the number of encrypted files
Serpent: 0.025/0.075 BTC

3.10. Targeted audience

This subsection suggests the target audience based on the language used in a web UI or ransom note.

VaultCrypt: Russian speaking (Russia, Ukraine)
TeslaCrypt: English speaking
NanoLocker: English speaking
Linux.Cryptor: English speaking
Simplelocker: Ukraine
OSX/KeRanger-A: English speaking
WannaCry: English speaking
Petya: English speaking
NotPetya: Ukraine
Cerber: English speaking
Spora: Russian speaking
Serpent: English speaking

3.11. Passive methods of protection

This subsection highlights the passive methods of self-protection used by ransomware.

VaultCrypt: n/a
TeslaCrypt: code obfuscation, traffic encryption
NanoLocker: packing, base64
Linux.Cryptor: n/a
Simplelocker: code obfuscation in some versions
OSX/KeRanger-A: packing
WannaCry: packing, encryption
Petya: n/a
NotPetya: n/a
Cerber: obfuscation, encryption
Spora: obfuscation, encryption
Serpent: obfuscation, encryption

3.12. Active methods of protection

This subsection highlights the active methods of self-protection used by ransomware.

VaultCrypt: n/a
TeslaCrypt: terminates msconfig, regedit, procexp, taskmgr tools
NanoLocker: n/a
Linux.Cryptor: n/a
Simplelocker: n/a
OSX/KeRanger-A: n/a
WannaCry: n/a
Petya: n/a
NotPetya: detects avp.exe (Kaspersky AV), NS.exe (Norton Security), ccSvcHst.exe (Symantec)
Cerber: n/a
Spora: n/a
Serpent: n/a

4. The results analysis

An analysis of the obtained results is presented below by the selected criteria.

4.1. Delivery method

Ransomware are delivered with the help of exploits and social engineering tricks. The methods include drive-by attacks when a compromised website is used to host an exploit represented as a malicious JavaScript. Or a spam message with a document containing the exploit. The malicious document has a fancy name and a double extension, for example 'Akt_Sverki_za_2014_year_Buhgalterija_SIGNED-ot_17.02_2015g_attachment.AVG.Checked.OK.pdf.js' [25].

4.2. File type

In addition to the ordinary executable file formats, we see more ransomware come as shell scripts. For example, VaultCrypt is as a Windows batch script and uses a standalone GnuPG tool [26] to encrypt files dropped from the delivered package.

4.3. Encryption

Most of cryptolockers use the AES block chaining encryption algorithm with the key length 128 or 256 bits due to performance issues. The only exception is VaultCrypt with RSA-1024 provided by GnuPG. After encryption is completed, the ransomware typically deletes the file encryption key from memory (TeslaCrypt) or file system (all others). Before that, the program usually encrypts the file's encryption key using asymmetric encryption algorithm such as RSA-1024 with the hard-coded master public key (an attacker owns the master private key) and is stored in a recovery message or key vault file to be uploaded to a decryption service. In the case of Android Simplelocker, the AES file encryption key is stored in the code, and it makes no problem to get encrypted data back.

In most of cases Microsoft Crypto Provider was used as available by default. Host intrusion prevention systems (HIPS) are aware of that, and provides monitoring of API calls for the presence of MS Crypto API calls. Therefore, some ransomware use alternative cryptolibraries (OpenSSL, PolarSSL, GnuPG) or come up with their own implementation to bypass HIPS protection.

When encrypting files cryptolockers may exclude locations where files should not be encrypted, such as system and home folders (VaultCrypt, TeslaCrypt, WannaCry, Cerber, Spora, Serpent), or, the other way around, the list of directories to be encrypted only (Linux.Cryptor). For example, Android Simplelocker encrypts files only on a phone's SD card.

Additionally, what was not mentioned in the analysis above, WannaCry and Serpent ransomware terminate database-related processes such as mysqld.exe, sqlwriter.exe, sqlserver.exe to unlock database files for encryption.

4.4. Deleting backups

Windows ransomware OSX/KeRanger-A, WannaCry, Spora, and Serpent delete backups of files using available system tools such as wmic.exe and vssadmin.exe together with cipher.exe used to wipe the deleted original files from the disk. OSX/KeRanger-A encrypts the Time Machine backup files. Thus, a user cannot restore original files and keys after the encryption has been finished.

4.5. Communication with a C&C Server

Commonly, ransomware send check-in requests in an encrypted way to an attacker's server via HTTP protocol. However, NanoLocker sends specially crafted ICMP packets to the remote server including a bitcoin address. Linux.Cryptor and Petya (NotPetya) does not communicate with a C&C server at all. Cerber and Spora can work even if a C&C server is offline. Serpent and Locky [27] ransomware require a connection to C&C to retrieve the master public RSA key to start encryption.

4.6. Decryption Service

A web decryption service is usually located in Tor network making it impossible to shut down or trace a master. The NanoLocker's master uses the Public Note in Bitcoin transaction to get the victim's encrypted key and to send back the decrypted one. Simplelocker has the C&C in Tor network, but the decryption function is available in its code.

4.7. Payment

A ransom is paid using anonymous payment services. Payments in Bitcoins are mostly used.

4.8. Targeted audience

Ransomware are widespread in Russian speaking region, mostly Russia and Ukraine. However, most of ransomware have an English user interface covering users from all over the world.

4.9. Passive and active methods of ransomware self-protection

Like other malware, cryptolockers use passive methods of protection: packing, obfuscation, and encryption. For example, TeslaCrypt uses 'push-ret' x86 ASM instructions instead of the normal 'call' instruction to call Windows API functions. The code snippet for IsDebuggerPresent() WinAPI call is shown in Figure 1.

```
inc     edx
sbb     eax, ebx
sbb     eax, ebx
sbb     ecx, edx

loc_B208DA:
and     edx, ebx
inc     edx
sbb     ecx, edx
inc     edx
popa
push    offset kernel32_IsDebuggerPresent
retn
```

Figure 1: Example of the obfuscated function call in TeslaCrypt 2.1 [2]

The same TeslaCrypt used active methods of protection in the form of terminating the Windows monitoring and configuration tools: task manager, process explorer, registry editor, and msconfig. The code is shown in Figure 2.

```
push    eax
call    GetProcessNameToCheck
lea     ecx, [ebp-2004h]
push    offset aTaskmgr                 ; "taskmgr"
push    ecx
call    ebx
add     esp, 10h
test    eax, eax
jnz     short loc_41F90B
lea     edx, [ebp-2004h]
push    offset aProcexp                 ; "procexp"
push    edx
call    ebx
add     esp, 8
test    eax, eax
jnz     short loc_41F90B
lea     eax, [ebp-2004h]
push    offset aRegedit                 ; "regedit"
push    eax
call    ebx
add     esp, 8
test    eax, eax
jnz     short loc_41F90B
lea     ecx, [ebp-2004h]
push    offset aMsconfig                ; "msconfig"
```

Figure 2: TeslaCrypt terminates Windows monitoring tools [2]

EternalPetya verifies if the antivirus processes are running on the infected host and does not run the encryptor.

5. Outcomes and mitigation recommendations

The analysis of ransomware presented in this paper helped to reveal trends in the evolution of ransomware and develop mitigation techniques to protect users from a crypto attack that violate information availability in this case.

Delivery method. The ransomware is being delivered through the Web and Email channels use the same propagation techniques as targeted attacks: web exploits and social engineering tricks. Moreover, recently ransomware started using exploits in SMB1 released by ShadowBrokers such as EternalBlue and EternalRomance to propagate.

To block ransomware on arrival, it is recommended:

- set up spam filters to quarantine suspicious emails and send attachments for advanced inspection in a malware sandbox;
- use an exploit execution prevention module and regularly consume the latest threat intelligence to prevent execution of exploits in a user's system.

In future, ransomware may start using 0-day exploits as well.

Encryption. If an attack is stopped before encryption is completed, a user has a chance to get a file encryption key stored in a file system or memory. The

encryption process can be interrupted by simply hibernating a system.

To block ransomware when ransomware starts encryption, it is recommended:

- to define additional trust boundaries in an operation system that will help block an cryptolockers accessing shared folders and network drives;
- deploy HIPS and regularly consume the latest threat intelligence to prevent execution of cryptolockers in a user's system.

Deleting backups. As a ransomware uses standard administration tools to erase shadow copies of files or wipe data from a disk, those can be blacklisted by configuring a local system security policy. The typical mistake is using a domain user's account to grant access to a file server or working under a local admin account.

Communication. Ransomware may encrypt their traffic and use standard network protocols making it hard to detect. However, it is possible to trace traffic to Tor network and notify a network administrator who can quarantine or even freeze a host that generates such a traffic.

Payment. Bitcoin payment system being anonymous becomes more and more popular among criminals [28, 29]. Even though, operations with bitcoins are restricted in the most of stock markets and depend mostly on particular country laws, victims can still buy Bitcoins from private persons on the black market. In Sweden, for example, bitcoins are treated as regular currency [30]. It is possible to buy and sell goods on the Internet using bitcoins. The Swedish government looks at big transactions only to prevent money laundering. However, most of ransom payments rarely exceed 2 BTC.

Targeted audience. Despite the most of ransomware were created by the Russian speaking developers based on artifacts found in the code, their user interfaces are available in English.

Passive and active ransomware self-protection. While passive methods such as obfuscation and encryption are used by many types of malware for a while, the active methods introduced first by TeslaCrypt shows the new trend in ransomware development. Once infected, it is hard to terminate a malicious process or make a dump to extract the session encryption key.

The research is still ongoing, and new versions of ransomware will be included as they have been discovered by our lab or antivirus companies.

6. References

[1] Young A., Yung M., Cryptovirology: Extortion-based security threats and countermeasures. In Security and Privacy Proceedings, IEEE Symposium, 1996, pp. 129–140.

[2] Young A. Building a Cryptovirus Using Microsoft's Cryptographic API. In Proceedings of the International Conference on Information Security, 2005, pp. 389–401.

[3] Kamluk V., GpCode-like Ransomware Is Back, Kaspersky Lab, https://securelist.com/blog/research/29633/gpcode-like-ransomware-is-back/ (2010)

[4] Upadhyaya R., Jain A., Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet, 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016, pp. 143-148

[5] Owen G., Savage N., Empirical analysis of Tor Hidden Services, IET Information Security, Volume 10, Issue: 3, 2016, pp. 113-118.

[6] Adamov A., Carlsson A, TeslaCrypt 2.1 Analysis: Cracking "Ping" Message, NioGuard Security Lab, 2015 http://nioguard.blogspot.com/2015/09/teslacrypt-21-analysis-cracking-ping.html

[7] Kharraz A., Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks, Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), Milan, Italy, July 9-10, 2015.

[8] New variant of Cerber ransomware (Ferber) analyzed, Nioguard Security Lab, July 2017, available at https://nioguard.blogspot.com/2017/07/new-variant-of-cerber-ransomware-ferber.html

[9] Spora Ransomware Analysis, Nioguard Security Lab, August 2017, https://nioguard.blogspot.com/2017/08/spora-ransomware-analysis.html

[10] Serpent Ransomware Analysis, Nioguard Security Lab, August 2017, https://nioguard.blogspot.com/2017/08/serpent-ransomware-analysis.html

[11] Petya – Taking Ransomware To The Low Level, MalwareBytes, April 2016, available at https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/

[12] Berry A., Homan J., Eitzman R., WannaCry Malware Profile, FireEye, May 2017,

https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html

[13] EternalPetya / NotPetya Ransomware Analysis, Nioguard Security Lab, June 2017, available at https://nioguard.blogspot.com/2017/06/eternalpetya-ransomware-analysis.html

[14] Adamov A., VaultCrypt: From Russia with Love, NioGuard Security Lab and Ukrainian Cyberpolice, 2015, http://nioguard.blogspot.com/2015/12/vaultcrypt-from-russia-with-love.html

[15] NanoLocker - Ransomware analysis, Malware Clipboard, http://blog.malwareclipboard.com/2016/01/nanolocker-ransomware-analysis.html (2016)

[16] Linux.Encoder.1, DrWeb, 2015, https://vms.drweb.com/virus/?i=7704004&lng=en

[17] ELF_CRYPTOR.A, TrendMicro, 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/elf_cryptor.a

[18] ESET Analyzes Simplocker – First Android File-Encrypting, TOR-enabled Ransomware, ESET, 2014 http://www.welivesecurity.com/2014/06/04/simplocker/

[19] Claud Xiao, Jin Chen, New OS X Ransomware KeRanger Infected Transmission BitTorrent Client Installer, Palo Alto Networks, March 2016, available at https://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/

[20] Howard F., A closer look at the Angler exploit kit, Sophos, 2015, https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/

[21] SDelete Tool, MSDN, https://support.microsoft.com/en-us/kb/315672

[22] Cipher tool, MSDN, https://technet.microsoft.com/en-us/library/bb490878.aspx

[23] VSSadmin Tool, MSDN, https://technet.microsoft.com/en-us/library/bb491031.aspx

[24] WMI command line interface, Microsft, https://msdn.microsoft.com/ru-ru/library/aa394531(v=vs.85).aspx

[25] VaultCrypt sample analysis, Virustotal, https://www.virustotal.com/en/file/6cceeddc0c631484f12f636aa9cdc9020c471af65a524423032e46e82004e179/analysis/

[26] GnuPG Tool, https://www.gnupg.org/

[27] Hasherezade, Look Into Locky Ransomware, MalwareBytes, July 2016, available at https://blog.malwarebytes.com/threat-analysis/2016/03/look-into-locky/

[28] Meiklejohn S. et al., A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Conference on Internet Measurement Conference, 2013, IMC '13, pp. 127–140.

[29] Fergal R., Martin H., An analysis of anonymity in the bitcoin system. In Security and Privacy in Social Networks, 2012.

[30] Swedish Bitcoin webportal, http://www.bitcoin.se/